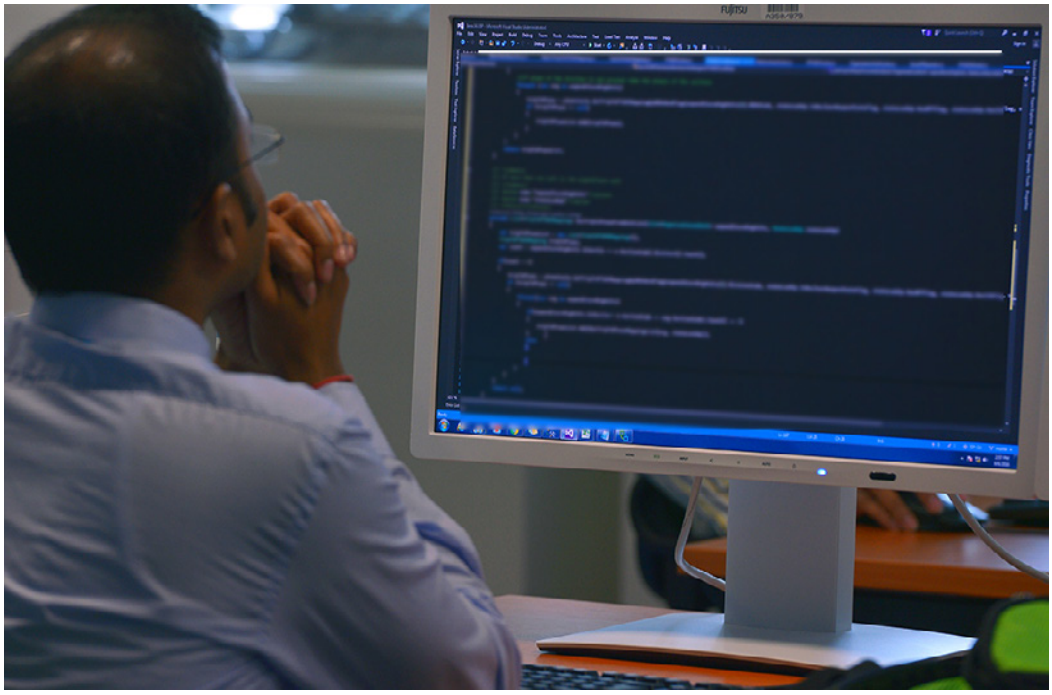
Armas, guardias, puertas y genios de la informática: Rumania refuerza la seguridad informática en las instalaciones nucleares

Laura Gil



(Fotografía: D. Calma/OIEA)

Un ciberataque puede robar toda la información almacenada en su computadora o incluso impedir que funcione. Por si esto fuera poco, un ciberataque contra una central nuclear podría dar lugar al sabotaje o el robo de materiales nucleares. La seguridad informática, que se ocupa de la protección de los datos digitales y de la defensa de los sistemas y redes contra actos dolosos, es un componente esencial de la seguridad física nuclear.

"Los progresos de las computadoras y su empleo en todos los aspectos de las operaciones nucleares han cambiado el paradigma de la seguridad física", nos dice Donald Dudenhoeffer, Oficial de Seguridad de la Tecnología de la Información del OIEA. "La seguridad de la información y la seguridad informática deben ser consideradas componentes del plan general de seguridad física nuclear."

En la seguridad física nuclear ha prevalecido durante mucho tiempo la protección física —denominada a menudo "armas, guardias y puertas"—, mas hoy día los delincuentes también emplean las computadoras como instrumento y objeto de sus ataques. Un ciberataque puede dar lugar a la pérdida de información relativa a la seguridad física nuclear, al sabotaje de instalaciones nucleares y, combinado con un ataque físico, al robo de materiales nucleares u otros materiales radiactivos. Las computadoras desempeñan actualmente un papel esencial en la seguridad tecnológica y física y la gestión de las instalaciones nucleares; es de importancia vital que todos los sistemas estén protegidos adecuadamente contra las intrusiones dolosas.

"Todos tenemos que estar preparados para defendernos del entorno no benigno de la Internet y la era digital", afirma el Sr. Dudenhoeffer. "Todos utilizamos computadoras y todos tenemos que ser más conscientes de las amenazas, los riesgos y los medios de protección." Los reguladores y los explotadores de instalaciones nucleares son cada vez más conscientes de la importancia de la seguridad informática y se esfuerzan en mejorar sus programas de seguridad física nuclear. Rumania, según el Sr. Dudenhoeffer, es un caso ejemplar.

"Entendemos la importancia de la protección contra toda clase de amenazas que puedan afectar a la explotación tecnológica y físicamente segura y fiable de nuestras instalaciones nucleares, comprendidas las amenazas dirigidas contra la seguridad informática y de la información", declara Madalina Tronea, Coordinadora de la Dependencia de Reglamentos y Normas Nucleares de la Comisión Nacional de Control de Actividades Nucleares (CNCAN) de Bucarest (Rumania).

En 2012, un grupo de especialistas del OIEA llevó a cabo una misión del Servicio Internacional de Asesoramiento sobre Protección Física en Rumania. Entregaron a las autoridades una lista de recomendaciones para perfeccionar el marco de reglamentación apropiado para la protección de las instalaciones nucleares contra diversas amenazas, entre ellas los ciberataques.

Poco después, un grupo de reguladores nucleares de la CNCAN empezó a trabajar en un reglamento que entró en vigor en noviembre de 2014, el cual trata de la protección de los sistemas, el equipo y los componentes —incluidos los programas informáticos de los sistemas de instrumentación y control— que son importantes para la seguridad nuclear tecnológica y física, las salvaguardias y la respuesta para casos de emergencia. Además del reglamento, la CNCAN publicó un documento en el que se exponen a grandes rasgos los ciberataques, teniendo en cuenta nuevas amenazas y sucesos recientes relativos a la seguridad informática acaecidos en la industria en todo el mundo.

"Prestamos atención al contexto mundial y a los cambios que experimentan las amenazas y las contramedidas", dice la Sra. Tronea. "Y hacemos todo lo posible para alcanzar una prevención y una protección adecuadas contra incidentes que afectan a la seguridad informática, así como una respuesta eficaz a esos incidentes, en caso de que se produzcan."

Ese mismo año, el Gobierno rumano aprobó una Estrategia Nacional de Seguridad Nuclear Tecnológica y Física, que contiene objetivos consagrados a la mejora permanente de la seguridad informática en el sector nuclear.

Las personas: el problema y la solución

Diversos estudios demuestran que la causa de la mayoría de los incidentes relacionados con la seguridad informática son los errores humanos.

"Las personas: el desarrollo de la capacidad humana es uno de los campos en que es más rentable invertir", asegura el Sr. Dudenhoeffer. "No necesitamos un mundo repleto de expertos en seguridad informática. Lo que nos hace falta es un mundo en el que las personas tengan conciencia de los riesgos que existen para la seguridad informática y de las medidas elementales de defensa. Nos hacen falta unos trabajadores y unos líderes bien informados."

(Fotografía: CNCAN)

Gracias a los cursos de capacitación del OIEA en los que Rumania ha participado desde 2013, el país ha creado una red sostenible de interesados directos en la cuestión. A través de ella, ahora comparten experiencias en materia de seguridad informática y trabajan aunados para concebir programas de seguridad de la información e informática robustos.

Por medio de cursos de capacitación nacionales, aprendizaje en línea, reuniones de expertos y programas de formación de capacitadores, el OIEA trabaja con los dirigentes de los países y las partes interesadas de la industria nuclear para comprender mejor las ciberamenazas y concebir buenas prácticas que mejoren la seguridad informática. Los cursos de capacitación nacionales, dice Dudenhoeffer, son unas de las actividades más valiosas que realiza el OIEA acerca de la seguridad informática.

"En la protección física, se puede ver lo que se protege y visualizar hipótesis de ataques probables", añade. "En el ciberespacio, en cambio, los delincuentes tienen muchos más blancos, entre ellos los que no se encuentran en la instalación; pueden incluso atacar a domicilio. Debemos aprender a pensar como los delincuentes para entender mejor cómo protegernos de los ciberataques dondequiera que estemos."